CONTRATO Nº 27/2022

PROCESSO LICITATÓRIO Nº 007/2022

PREGÃO PRESENCIAL Nº 007/2022

A **CÂMARA MUNICIPAL DE ITABIRITO**, CNPJ 18.366.963/0001-79, Inscrição Estadual: Isento, com sede administrativa na Avenida Queiroz Júnior, nº 639, Bairro Praia, Itabirito/MG, CEP: 35.450-228, telefone: (31) 3561-1599, representada pelo Presidente, Vereador **ARNALDO PEREIRA DOS SANTOS**, portador do CPF nº e da Carteira de Identidade nº , expedida pela SSP/MG, residente e domiciliado em Itabirito/MG, a seguir denominada CONTRATANTE e a empresa **BRAGA & FONTES INFORMÁTICA LTDA** inscrita no CNPJ sob o nº 07.074.778/0001-94 , estabelecida na Rua Três Pontas, 979 2º andar, sala 01 Bairro Carlos Prates, Belo Horizonte/MG . CEP:30.710.560 , neste ato representada por **PRESLEYSON PLÍNIO DE LIMA** portador do CPF nº , doravante denominada CONTRATADA, resolvem firmar o presente contrato, como especificado no seu objeto, em conformidade com o Processo Licitatório nº 007/2022, na modalidade Pregão Presencial nº 007/2022, do tipo menor preço por item, de acordo com as Leis nºs 10.520/2002 e 8.666/93 e suas posteriores alterações, pela Lei Complementar nº 123/2006, atualizada pela Lei Complementar nº 147/2014, pelo Decreto nº 3.555/2000, pelo Decreto Municipal no 8949/2010, alterado pelo Decreto Municipal 9345/2011 e pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

Este Contrato tem como objeto a **contratação de pessoa jurídica para fornecimento de solução LICENÇA SOFTWARE ANTIVÍRUS**, **para atender a Câmara Municipal de Itabirito/MG, conforme especificações abaixo:**

Contratação de pessoa jurídica para fornecimento de solução LICENCA SOFTWARE ANTIVIRUS, para servidores e estações de trabalho com console de gerenciamento compatível com os sistemas operacionais Windows Server 2008 R2, 2012, 2016 e 2019 e Linux. A solução deve apresentar, minimamente, os seguintes elementos: console de gerenciamento, atualização de vacinas, cliente gerenciado, funcionalidades de firewall, IPS, antimalware, reconhecimento de novas ameaças, controle de dispositivos, controle de aplicação e relatórios, descrição detalhada conforme anexo I do Edital.

Item	Qtde.	Un	Período	Descrição	marca	Valor Total
1	120	Licença	36 meses	Aquisição de licenças, para instalação, suporte técnico, gerenciamento centralizado e atualização de software Antivírus do tipo “Proteção de Endpoint”	Sophos	14.400,00

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

CLÁUSULA SEGUNDA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

2.1- A Câmara reserva-se no direito de não aceitar o objeto em desacordo com o previsto neste instrumento convocatório, podendo rescindir o contrato nos termos do art. 78, inciso I, e aplicar o disposto no art. 24, XI, ambos da Lei nº 8.666/93.

2.2- A Câmara Municipal fiscalizará o objeto desta licitação, observados os artigos 67 a 70 e 73 a 76 da Lei nº 8.666/93.

2.3- A gestora e fiscal do contrato e ata será a servidora Layane Cristine Pedro de Faria.

2.4- As decisões, comunicações, ordens ou solicitações deverão se revestir, obrigatoriamente, da forma escrita e obedecer às normas emanadas por esta Câmara.

2.5- A fiscalização do fornecimento pela Contratante não exclui a responsabilidade da Contratada por qualquer inobservância ou omissão à legislação vigente e às cláusulas contratuais do objeto do Contrato.

2.6- A Contratada é obrigada a assegurar e facilitar o acompanhamento do fornecimento pela Contratante, bem como permitir o acesso a informações consideradas necessárias.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DAS PARTES

São obrigações das partes, além de outras previstas no Edital e Anexos:

3.1- DA CONTRATADA:

O prazo de vigência do contrato será de 36 (trinta e seis) meses, tendo início a partir da data de sua assinatura.

A Contratada deverá disponibilizar link e/ou respectivo(s) arquivo(s) para downloads para a devida execução do contrato em até 10 (dez) dias após o recebimento da ordem de serviço.

As licenças deverão ter validade de 36 meses.

O Contrato firmado com a Câmara Municipal não poderá ser objeto de cessão, transferência ou subcontratação, sob pena de aplicação de sanção, inclusive rescisão.

A Contratada deverá seguir rigorosamente as normas e padrões estabelecidos em lei, bem como diligenciar para que o fornecimento seja feito em perfeitas condições, não podendo conter quaisquer vícios.

Especificações técnicas:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- Console de gerenciamento centralizada.

- O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.
- O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.
- O acesso ao Console deve suportar várias sessões simultâneas.
- Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.
- Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.
- Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.
- O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases e Hypervisors:
  a) Microsoft Windows 8 / 8.1 Pro;
  b) Microsoft Windows 10;
  c) Microsoft Windows Server 2012 R2;
  d) Microsoft Windows Server 2016;
  e) Microsoft Windows Server 2019;
  f) Ubuntu 16.04.1 LTS x86 Desktop;
  g) Ubuntu 16.04.1 LTS x86 Server;
  h) Ubuntu 16.04.1 LTS x64 Desktop;
  i) Ubuntu 18.04.1 LTS x64 Desktop;
  j) Ubuntu 18.04.1 LTS x64 Server;
  k) Ubuntu 20.04 LTS x64;
  l) RHEL Server 7 x64;
  m) RHEL Server 8 x64;
  n) CentOS 7 x64;
  o) CentOS 8 x64;
  p) SLED 15 x64;
  q) SLES 11 x64;
  r) SLES 12 x64;
  s) SLES 15 x64;
  t) OpenSUSE Leap 15.2 x64;
  u) Debian 9 x64;
  v) Debian 10 x64;
  w) Fedora 31 x64;
  x) Fedora 32 x64;
  y) VMware vSphere/ESXi 6.5 e posterior;
  z) VMware Workstation 9 e posterior;
  aa) VMware Player 7 e posterior;
  bb) Microsoft Hyper-V Server 2012, 2012 R2, 2016, 2019;
  cc) Oracle VirtualBox 6.0 e posterior;
  dd) Citrix 7.0 e posterior;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE.
- Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.
- Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.
- Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.
- Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).
- Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.
- Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.
- Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.
- A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.
- Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).
- O log deve ser centralizado e conter, no mínimo, os seguintes itens:
  a) Nome da ameaça;
  b) Nome do arquivo infectado;
  c) Data e hora da infecção;
  d) Ação tomada;
  e) Endereço de IP da máquina;
  f) Usuário autenticado na máquina;
  g) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;
- O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques.
- Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.
- Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.
- Interface da Console de Gerenciamento totalmente em português.
- Possuir manuais em português e inglês.
- O fabricante deverá ter documentação publicada na internet no idioma português.
- Deve permitir criar o backup da Base de dados da Console de gerenciamento.
- O acesso a console de gerenciamento deverá ser autenticado.
- A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- O console de administração de licenças deve ser na nuvem, aonde é possível revisar os detalhes dos equipamentos que estão utilizando a licença do antivírus.
- O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da mesma console aonde é possível ativá-lo sem a necessidade de nenhum add-on adicional.
- Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.
- Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.
- Atualização de vacinas sem a necessidade de reinicialização.
- Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.
- Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.
- Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP;
- Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.
- Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.
- Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.
- Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.
- Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.
- Possuir no mínimo 42 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.
- Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles):

a) HTML;
b) CSV ou TXT;
c) PDF;

- Geração de relatórios que contenham as seguintes informações:

a) Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus;
b) Versão do software instalado em cada máquina;
c) Vírus que mais foram detectados;
d) Máquinas que mais sofreram infecções em um determinado período de tempo;

- Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

a) Registro de eventos (log);
b) Relatórios de eventos de vírus e status dos clientes;
c) Relatórios de Softwares instalados;
d) Relatórios de Hardware encontrados;

- Fornecer, em tempo real, o status atualizado das estações de trabalho;
- Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.
- Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

a) Machine Learning
b) Instrusion Prevention System
c) Inteligência Artificial

- Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.
- Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.
- Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.
- Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.
- Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.
- Por meio do console de gerenciamento deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.
- O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.
- O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.
- A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso.
- A solução deve possuir um cache local para aumentar o desempenho dos ambientes virtuais, garantindo que o arquivo seja verificado apenas uma vez.
- Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.
- Atualização incremental e on-line das vacinas.
- Atualização em clientes móveis (notebook, laptop, netbook, ultrabook, e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.
- Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.
- Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.
- Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.
- Qualquer atualização deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la.
- Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.
- O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.
- O fabricante deve possuir mais de 70 prêmios no VB100 do Virus Bulletin e o mínimo de 80 participações no mesmo.

- Solução de Antivírus para as estações e servidores.

- A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.
- Gerenciado através de Console de Gerenciamento.
- Interface do software cliente em português.
- Manuais em português.
- O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:
  a) Microsoft Windows 7;
  b) Microsoft Windows 8;
  c) Microsoft Windows 8.1;
  d) Microsoft Windows 10;
  e) Microsoft Windows 2008 server;
  f) Microsoft Windows 2008 R2 server;
  g) Microsoft Windows 2012 R2 server e/ou superior;
  h) Red Hat;
  i) SUSE;
  j) Ubuntu;
  k) CentOs;
  l) Debian;
  m) Fedora;
  n) MacOS 10.12 Sierra;
  o) MacOS 10.13 High Sierra;
  p) MacOS 10.14 Mojave;
  q) MacOS 10.15 Catalina;
  r) Android 5 e versões posteriores;
  s) IOS 9 e versões posteriores.
- O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.
- Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail.
- O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.
- Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.
- Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.
- Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.
- O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.
- Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.
- Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (PATCHES) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalado/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning) capaz de identificar e bloquear qualquer ameaça externa que utilize-se de vulnerabilidades dos sistemas operacionais.
- Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.
- A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:
  a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).
  b) Pastas e arquivos pré determinados através do caminho ou Hash.
- Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.
- Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.
- Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos na console de gerenciamento centralizada:
  a) Permitir atualização incremental da lista de definições de vírus;
  b) Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;
  c) Permitir configuração remota de ordem de preferência de endereços de atualização;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

d) Permitir configurar conexão através de serviço Proxy local;
e) Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;

- No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.
- Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.
- Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.
- Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.
- Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.
- Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.
- Rastreamento manual com interface gráfica, customizável, com opção de limpeza.
- Rastreamento por linha de comando, parametrizável, com opção de limpeza.
- Programação de rastreamentos automáticos do sistema com as seguintes opções:
  a) Escopo: todos os drives locais, específicos ou pastas específicas;
  b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;
  c) Frequência: diária, semanal e mensal;
  d) Exclusões: pastas ou arquivos que não devem ser rastreados.
- Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.
- Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.
- Proteção contra ameaças via internet. A solução deve conter pelo menos:
  a) Ajuste no nível de sensibilidade da detecção;
  b) Lista de exceção.
- Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.
- Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada;
- Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).

- Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.
- Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como:
  a) PenDrive
  b) HD externo
  c) Celulares
  d) Tablets
  e) CD/DVD
  f) Impressora USB
  g) Armazenamento de FireWire
  h) Dispositivo Bluetooth
  i) Leitor de cartão inteligente
  j) Dispositivo de criação de imagem
  k) Modem
  l) Porta LPT/COM
  m) Dispositivo portátil
- O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.
- Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.
- Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.
- A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.
- Deve permitir o bloqueio do “Autorun” nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.
- Permitir bloquear a conexão de dispositivos removíveis.
- Gerar registro (log) dos eventos de vírus em arquivo.
- Gerar relatórios, ao menos, de:
  a) Eventos de vírus;
  b) Status dos clientes;
  c) Status dos Updates;
- Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.
- Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.
- Fabricante deverá ter suporte local em idioma português.
- Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:
  a) Nome da máquina;
  b) Endereço IP da máquina;
  c) Malwares não removidos;
  d) Status da conexão;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

e) Data da vacina;
f) Versão do antivírus instalado.

- Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.
- Permitir a criação de exceções nos escaneamentos de arquivos.
- Permitir o bloqueio de dispositivos com base nos seguintes critérios:
  a) Fabricante
  b) Modelo
  c) Número de série
- Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.
- O Firewall deve possuir funcionalidade deve suportar os protocolos TCP e UDP.
- O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.
- Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.
- Possibilidades de criação de assinaturas personalizadas para detecção.
- Possibilidade de agendar a ativação de novas regras do firewall.
- Possibilidade de criar regras diferenciadas por aplicações.
- Possibilidade de criar regras para bloqueio de todos os executáveis da lista ou liberar somente os executáveis da lista.
- Bloqueio de ataques baseado na exploração da vulnerabilidade.
- Permitir integração com navegadores WEB para prevenção de ataques.
- Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.
- Possuir taxa de performance de rede inferior a 70MB (mega bytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.
- O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a pesquisa de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.
- O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.
- Tenha escritório do fabricante no Brasil.
- O fabricante não deve possuir nenhum falso positivo nas provas realizadas pelo VB100 do Virus Bulletin nos últimos dez anos.
- O fabricante deve ser citado nos relatórios do MITRE ATT&CK como contribuinte de informações e técnicas de detecção nos últimos anos.
- A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.
- As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução.
- Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.
- Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.
- Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.
- Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.
- Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.
- Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:
  a) CAB;
  b) ZIP;
  c) RAR;
  d) LHA;
  e) ARJ;
  f) TAR;
- Capacidade de terminar o processo e serviço da ameaça no momento de detecção.
- Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.
- Possibilidade de bloquear verificação de malware em recursos mapeados da rede.
- Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.
- Não serão aceitas soluções de Antimalware que possuam engine de terceiros.
- Permitir o bloqueio da execução de aplicações baseado em nome e pasta.
- A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.
- Capacidade de detecção de keyloggers por comportamento dos processos em memória.
- Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.
- Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.
- Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:
  a) Aprendizado de máquina;
  b) Deep Learning;
  c) Análise estatística e dinâmica;
  d) Detecção baseada em comportamento;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

e) Introspecção na memória;

- Detecção do malware por DNA do vírus.
- O fabricante deve possuir uma posição de Challenger no Quadrante Mágico do Gartner no último ano.
- Deverá ter a capacidade de atualizar os patches do sistema operacional.
- A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hipervisor.
- Em servidores que usam “OneDrive for Business” você deve explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.
- A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.
- A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.
- Otimize o desempenho de infraestruturas mistas (hardware e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.
- Controlar acesso a sites, possibilitando o bloqueio do mesmo.
- Permitir criar políticas de bloqueio com base em categorias e lista de URL.
- Permitir gerar relatórios de sites acessados e bloqueados.
- Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.
- Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.
- Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.
- A solução de proteção Antispam deve realizar as verificações utilizando o protocolo SSL.
- Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push (EPNS).

O recebimento definitivo dos produtos se dará em até 10 (dez) dias após a conferência e verificação das licenças e sua conformidade com a quantidade, especificações, marca e preço, certificando-se de que todas as condições estabelecidas foram atendidas.

O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do fornecimento, nem a ético-profissional, pela perfeita execução do contrato.

A justificativa de quaisquer atrasos no cumprimento dos prazos previstos acima somente será considerada se apresentada por escrito, e após aprovação da Câmara Municipal de Itabirito.

A tolerância com qualquer atraso ou inadimplemento por parte da contratada não importará, de forma alguma, em alteração contratual ou renovação, podendo a solicitante exercer seus direitos a qualquer tempo.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

A Contratada obriga-se a manter, durante toda a vigência do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar à contratante, imediatamente, qualquer alteração que possa comprometer a manutenção do contrato.

A Contratada deverá ser responsável pelo pagamento de todos os encargos, tributos, frete, licenças, alvarás, taxas e quaisquer outras contribuições que sejam exigidas para o fornecimento.

A Contratada assumirá inteira responsabilidade pelas obrigações decorrentes da legislação trabalhista, previdenciária de acidentes de trabalho e quaisquer outras relativas a danos a terceiros.

A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem no fornecimento, até 25% (vinte e cinco por cento) de acordo com o que preceitua o art. 65, § 1º, da Lei nº 8.666/93.

O Contrato não estabelece qualquer vínculo de natureza empregatícia ou de responsabilidade entre a CONTRATANTE e os agentes, prepostos, empregados ou demais pessoas da CONTRATADA designadas para a execução do objeto, sendo a CONTRATADA a única responsável por todas as obrigações e encargos decorrentes das relações de trabalho entre ela e seus profissionais ou contratados, previstos na legislação pátria vigente, seja trabalhista, previdenciária, social, de caráter securitário ou qualquer outra.

A CONTRATADA, por si, seus agentes, prepostos, empregados ou qualquer encarregado, assume inteira responsabilidade administrativa, civil e criminal, por quaisquer danos ou prejuízos causados, direta ou indiretamente, à CONTRATANTE, seus servidores ou terceiros, produzidos em decorrência da execução do objeto deste Contrato, ou da omissão em executá-lo, resguardando-se à CONTRATANTE o direito de regresso na hipótese de ser compelido a responder por tais danos ou prejuízos.

O atraso ou a abstenção pela CONTRATANTE, do exercício de quaisquer direitos ou faculdades que lhe assistam em decorrência da lei ou do presente contrato, bem como a eventual tolerância com atrasos no cumprimento das obrigações assumidas pela CONTRATADA não implicarão em novação, não podendo ser interpretados como renúncia a tais direitos ou faculdades, que poderão ser exercidos, a qualquer tempo, a critério exclusivo da Administração.

3.2- DA CONTRATANTE:

Acompanhar e supervisionar a execução do objeto pela CONTRATADA.

Fornecer subsídios e informações necessárias a execução do objeto.

Efetuar o pagamento da forma pactuada.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Notificar a Contratada, fixando-lhe prazo para corrigir defeitos ou irregularidades encontrados na execução do objeto.

CLÁUSULA QUARTA: DO VALOR E DAS CONDIÇÕES DE PAGAMENTO

4.1- O valor total do presente contrato é de R$ 14.400,00 (quatorze mil e quatrocentos reais)

4.2- O pagamento será realizado até o décimo dia após o fornecimento e apresentação da respectiva Nota Fiscal, devidamente conferida e assinada pela responsável pela fiscalização.

4.3- A nota fiscal/fatura deverá ser emitida pela própria Contratada, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e de proposta de preço e no próprio instrumento de Contrato, não se admitindo notas fiscais/faturas emitidas com outro CNPJ, mesmo que aquele de filial ou da matriz.

4.4- Para qualquer alteração nos dados da empresa, a Contratada deverá comunicar ao Contratante por escrito, acompanhada dos documentos alterados, no prazo de 15 (quinze) dias antes da emissão da Nota Fiscal.

4.5- A contratada deverá apresentar junto à nota fiscal cópia dos seguintes documentos: Certidões de Regularidade municipal, estadual, federal/INSS Unificada, trabalhista e CRF-FGTS.

4.6- Em caso de irregularidade da emissão da(s) nota(s) fiscal(is), o prazo de pagamento será contado a partir de sua reapresentação, desde que devidamente regularizada(s).

4.7- No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pela CONTRATANTE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

CLAUSULA QUINTA - DA DOTAÇÃO ORÇAMENTÁRIA

5.1- A dotação orçamentária destinada ao pagamento do objeto licitado será a abaixo indicada:

01.031.0001 2.006 – manutenção das atividades da Câmara Municipal
3.3.90.40.00.00 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica
Ficha 25

CLÁUSULA SEXTA: DO PRAZO

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

6.1- O prazo de vigência do contrato será de 36 (trinta e seis) meses, tendo início a partir da data de sua assinatura.

CLÁUSULA SÉTIMA: DAS SANÇÕES

7.1-Pela recusa injustificada em assinar o Contrato dentro do prazo estabelecido, multa de 5% (cinco por cento) sobre o valor da obrigação;

7.2-A penalidade prevista no subitem acima não se aplica às empresas remanescentes, em virtude da não aceitação da primeira convocada.

7.3-Pelo descumprimento total ou parcial das condições previstas nesse Edital, a Administração poderá, garantida a prévia defesa, aplicar à contratada as sanções previstas no art. 87 da Lei 8.666/93, sem prejuízo da responsabilidade civil e penal cabíveis:

7.4-Pelo atraso injustificado na execução do objeto:
a- Até 05 (cinco) dias - multa de 1% (um por cento) sobre o valor da obrigação, por dia de atraso;
b- Superior a 05 (cinco) dias - multa de 2% (dois por cento) sobre o valor da obrigação, por dia de atraso;
c- Pela inexecução total ou parcial do contrato - multa de 20% (vinte por cento), calculada sobre o valor das parcelas vincendas;

7.5-Advertência;

7.6-Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos, nos casos em que o convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

7.7-Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada.

7.8-As sanções previstas no item 7.4 poderão ser aplicadas juntamente com as demais penalidades, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

7.9-As Multas acima referidas serão descontadas dos pagamentos devidos à contratada. Na hipótese de não haver crédito suficiente à Contratada para quitar o valor total da multa, a diferença será cobrada mediante guia a ser emitida para este fim, ou por via judicial.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

7.10- O prazo para pagamento das multas será de até 05 (cinco) dias úteis a contar da intimação da empresa apenada.

CLÁUSULA OITAVA – DA RESCISÃO

8.1-Constituem motivos para rescisão do contrato os casos previstos nos arts. 77 e 78 da lei 8.666/93.

8.2-O contrato poderá ser rescindido na forma do art. 79 da Lei 8.666/93.

8.3-Em caso de rescisão prevista nos incisos XII a XVII do art. 78 da lei 8.666/93, sem que haja culpa da contratada, será esta ressarcida dos prejuízos regulamentares comprovados, quando os houver sofrido, tendo ainda direito à devolução de garantia, pagamentos devidos pela execução do contrato até a data da rescisão e pagamento do custo da desmobilização.

8.4-A rescisão contratual de que trata o inciso I do art. 79 acarreta as consequências previstas no art. 80, ambos da lei 8.666/93.

8.5-Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA NONA – DA REVISÃO DOS PREÇOS

9.1-Havendo alterações na conjuntura econômica do País ou do Estado, que resulte em desequilíbrio financeiro permanente, nas condições do contrato e nas hipóteses autorizadas pela Lei de Licitações, a Contratada poderá pleitear revisão de preços.

9.2-A revisão será aprovada conforme apresentação das Planilhas de Custos e/ou Nota Fiscal anterior ao processo do qual baseou o preço da proposta apresentada e a Nota Fiscal atual comprovando o preço a ser revisado. O preço poderá sofrer acréscimo como decréscimo de acordo com o preço praticado no mercado.

9.3-A cada pedido de revisão de preço deverá comprovar as alterações ocorridas e justificadoras do pedido, demonstrando novamente à composição do preço, através de notas fiscais que comprovem o aumento do preço.

9.4-É vedado à contratada interromper o fornecimento, sendo a contratada obrigada a continuá-lo enquanto aguarda o trâmite do processo de revisão de preços, estando neste caso sujeito às penalidades previstas neste edital.

9.5-A revisão levará em consideração preponderantemente as normas legais federais, estaduais e municipais.

CLÁUSULA DÉCIMA – DA VINCULAÇÃO CONTRATUAL

10.1- Este contrato está vinculado de forma total e plena ao **Processo Licitatório nº 007/2022**, **Pregão Presencial nº 007/2022,** que lhe deu causa, para cuja execução exigir-se-á rigorosa obediência ao Edital e seus Anexos.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

CLÁUSULA DÉCIMA PRIMEIRA - DO FORO

11.1- Fica eleito o foro da Comarca de Itabirito, Estado de Minas Gerais, para solucionar quaisquer questões oriundas desta licitação.

E, por estarem justas, as partes firmam o presente Contrato em 02 (duas) vias de igual teor e forma, na presença de duas testemunhas abaixo.

Itabirito, 20 de junho de 2022.

CÂMARA MUNICIPAL DE ITABIRITO
ARNALDO PEREIRA DOS SANTOS
Presidente da Câmara Municipal de Itabirito
Contratante

Contratada

_____	_____
Testemunha	Testemunha
CPF:	CPF:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br